(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35226 A1

(51) International Patent Classification[7]: G06F 12/14, 17/30

(21) International Application Number: PCT/SE00/02219

(22) International Filing Date:
13 November 2000 (13.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9904094-1 12 November 1999 (12.11.1999) SE

(71) Applicant *(for all designated States except US)*: PROTEGRITY RESEARCH & DEVELOPMENT [SE/SE]; Expolaris Center, S-931 78 Skellefteå (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: VALFRIDSSON, Thomas [SE/SE]; Rudagatan 69, S-931 53 Skellefteå (SE). MATTSSON, Ulf [SE/US]; 78 River Road A3, Um Cos Cob, CT 06807 (US).

(74) Agent: AWAPATENT AB; Box 11394, S-404 28 Göteborg (SE).

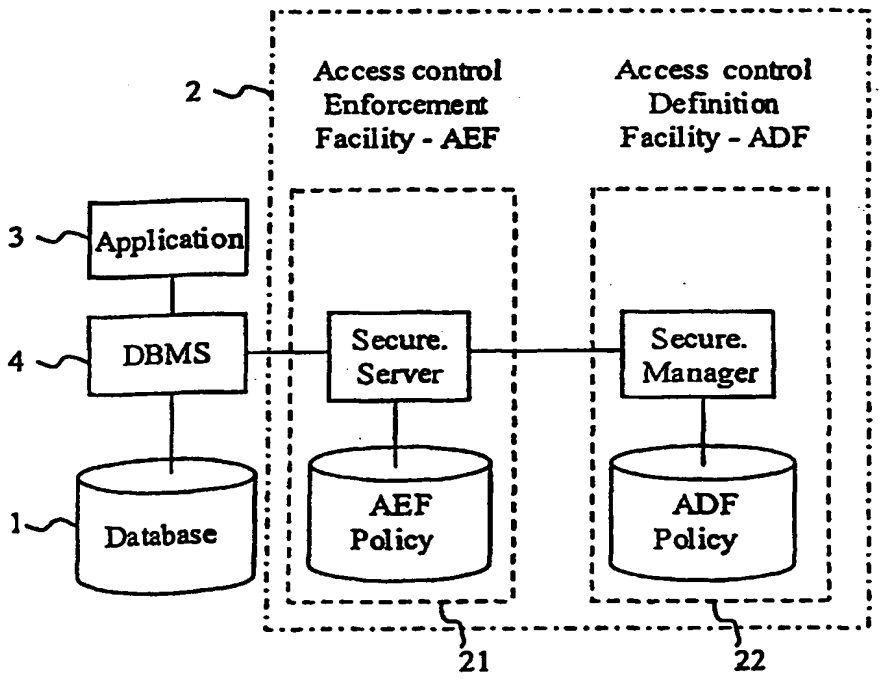
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR REENCRYPTION OF A DATABASE



(57) Abstract: The present invention relates to a method for encryption of the content in a database, for accomplishing increased protection against unauthorised access to the data. The method assures that every row and item is re-encrypted with a valid key. More specifically this process, the so-called KeyLife process, is executed every time a row is inserted, updated or retrieved after a scanning operation. The key life value, defining the number of days a key is valid for each item, could differ for the items, and could typically be between 30 and 90 days. The scanning operation, checking the validity of the presently used keys, the so-called KeyLife checking, is executed each time a new key generation is created.

WO 01/35226 A1

METHOD FOR REENCRYPTION OF A DATABASE

Field of the invention

The present invention relates to a method for encryption of the content in a database, for accomplishing increased protection against unauthorised access to the data.

Background of the invention

In order to protect information stored in a database, it is known to store sensitive data encrypted in the database. To access such encrypted data you have to decrypt it, which could only be done by knowing the encryption algorithm and the specific decryption key being used. The access to the decryption keys could be limited to certain users of the database system, and further, different users could be given different access rights.

Specifically, it is preferred to use a so-called granular security solution for the encryption of databases, instead of building walls around servers or hard drives. In such a solution, which is described in the document WO 97/49211 by the same applicant, a protective layer of encryption is provided around specific sensitive data-items or objects. This prevents outside attacks as well as infiltration from within the server itself. This also allows the system manager to define which data stored in databases are sensitive and thereby focusing the protection only on the sensitive data, which in turn minimizes the delays or burdens on the system that may occur from other bulk encryption methods.

Most preferably the encryption is made on such a basic level as in the column level of the databases. Encryption of whole files, tables or databases is not so granular, and does thus encrypt even non-sensitive data. It is further possible to assign different encryption

keys of the same algorithm to different data columns. With multiple keys in place, intruders are prevented from gaining full access to any database since a different key could protect each column of encrypted data.

However, there are problems with the previously known database encryption methods. Especially there is a problem to replace the old encryption keys in a 7 days by 24 hours operational database, since the database has to be taken out of operation when keys should be exchanged. Further, there is a problem accessing data for which the encryption keys have been exchanged.

Summary of the invention

It is therefore an object of the present invention to provide a method for encryption of the content in a database, for accomplishing increased protection against unauthorised access to the data.

This object is achieved with the method according to the appended claims.

Brief description of the drawings

For exemplifying purposes, the invention will be described in closer detail in the following with reference to embodiments thereof illustrated in the attached drawings, wherein:

Fig. 1 shows an example of a database system using the inventive method.

Description of preferred embodiments

Referring to fig 1, a database system according to the invention is illustrated, comprising at least one database 1, at least one security system 2, and at least one client 3. The database is operated through a database management system (DBMS) 4, which is a program providing the mechanisms and functionality for systematic storage and retrieval of data from the database. The DBMS could

be operated on a conventional personal computer, on a microcomputer or the like.

The security system 2 preferably comprises an access control enforcement facility (AEF) 21 and an access control definition facility (ADF) 22. The ADF provides security administration services and the AEF provides real-time enforcement of security parameters. The ADF 22 comprises a management system, Secure.Manager, and a memory for storing the ADF policy. ADF, the security administration services facility, preferably provides a complete RBAC facility, which using a drag and drop graphical user interface could enable the security administrator to create and maintain users, functional and organizational roles and their associated access privileges. The AEF 21 comprises a management system, "Secure.Server", and a memory for storing the ADF policy. AEF, the security enforcement services facility, is central to the architecture of the inventive method. In general it should receive security policy (and updates) via secure transmission from ADF. Further, it controls real-time access to all protected elements of the database 1 at the appropriate granularity.

The security system 2 could be operated on a conventional personal computer, on a microcomputer or the like. Further, it could be operated on the same computer as the DBMS, or on a separate computer connected to the DBMS computer by a data network.

In the database according to the invention a granular security solution is used, where the items of the database is individually encrypted. Further, information about the encryption keys used for the specific database item are stored in association with the item. Most preferably the encryption is made on such a basic level as in the column level of the databases. It is further possible to assign different encryption keys of the same algorithm to different data columns. With multiple keys in place, intruders are prevented from

gaining full access to any database since each column of encrypted data is protected by a different key.

The information about the encryption keys stored in association with the database items, e.g. database rows, could be provided by storage of a hash value of the encryption key together with the encrypted data for each row.

The data for each row and column is preferably stored together with an encryption key generation counter. The data for each row and column can be concatenated with the encryption key generation counter.

The databases could e.g. be Oracle 8.0.5 or Informix 9.14, but several other commercially available databases are possible to use for the inventive method. The platforms for the database system could e.g. be NT, HP-UX, Sun Solaris or AIX. The encryption algorithm used by the invention could e.g. be DES, and both software and hardware encryption could be used. More generally, the encryption used by the invention may concern any form of encryption, and is especially to concern methods of conversion including hashing.

According to the inventive method the encryption keys are replaced and updated automatically. This is achieved by defining a length of a time period to be used, deciding, for each time period at least one encryption key to be used when entering new database items to the database is decided, associating each encryption key with a life time value, and indicating the number of time periods during which the key will be valid. Hereby it is possible to scan the database to discover items with no longer valid encryption keys and replace such discovered invalid keys with keys assigned to the current time period.

Thus, the database reencrypt feature is based on multiple active keys and a timestamp for the last update time associated, preferably as a column or part of a data column, with each row or data item. Each key is

preferably unique for each item and generation of keys, i.e. keys generated during the same period. For example, the period P could be a week, whereby the key generation for week one in year 1999 could be identified as 199901. A new key generation is generated when a new period P starts.

Each key has a specific lifetime value L, stored in the database for the security system, i.e. the number of time periods during which the key is valid. The lifetime could vary between different keys.

The table of historic keys is preferably stored in the database for the security system. Storing the old keys enables decryption of historic generations of data.

Further, each item or row in the database comprises a timestamp indicating when it was last updated. Each row may contain columns encrypted with potentially different key generations.

When new items are entered into to the database for the current time period P is used, and for reading items from the database data is decrypted with the matching key of the active keys. When a new period is entered a key scan operation is started, preferably as a background process started. In this operation no longer valid keys are replaced by presently active keys. The key scan operation need not be started immediately after entering the new period, but is preferably executed as soon after the entrance as possible.

Example of an operational scenario

The method according to the invention will now be further described by way of an operational scenario. The time period P is here decided to be one week. Each row has a timestamp (week) for last update. Each key have a life time of L (weeks). A column C1 in the database could e.g. have the structure:

Column C1

Data Value A and encryption key generation counter
Data Value B and encryption key generation counter
Data Value C and encryption key generation counter

For an object I1 the key life L is decided to 2 weeks. Hence, after two weeks the active keys for object I1 will be from both key generation 1 and 2. If application data C is input to item 1 during week 1 and A and B during week 2 we will therefore have the following situation:

Column C1	TimeStamp (week)	KeyGen
A	2	2
B	2	2
C	1	1

When week 3 starts key generation 3 is created, and the table of active key generations for object I1 will now contain key generations 3 and 2. The table of historic keys for item 1 will contain key generation 1. At this time the application data of the first row in column C1 is updated, and the newly stored data will be encrypted by a key from the current key generation 3, whereby the following situation is achieved:

Column C1	TimeStamp (week)	KeyGen
A	3	3
B	1	2
C	1	1

However, the key scanning operation started at the beginning of period 3 will discover that the presence of a now non-valid key generation 1 for row C, and this key

will therefore be updated, providing the following situation:

Column C1	TimeStamp (week)	KeyGen
AA	3	3
B	2	2
C	3	3

When week 4 starts key generation 4 is created. The table of active key generations for object I1 will now comprise key generations 4 and 3, while the table of historic keys will comprise the key generations 2 and 1.

The application data after the key scanning operation and updating will be:

Column C1	TimeStamp (week)	KeyGen
AA	3	3
B	4	4
C	3	3

When week 5 starts the key life L for I1 is changed to 1 week. Further, key generation 5 is created. Due to the shorter key life, the table of active keys for item 1 will now only contain key generation 5, and the table of historic keys at the same time contain the key generations 4, 3, 2 and 1. After the key scanning and updating operations the application data situation for object I1 will be as follows:

Column C1	TimeStamp (week)	KeyGen
AA	5	5
B	5	5
C	5	5

When week 6 starts key generation 6 is created, and the table of active keys for item 1 will now contain key generation 6, and the table of historic keys the key generations 5, 4, 3, 2 and 1. If the item in the second row, B, is now updated the following situation will be achieved:

Column C1	TimeStamp (week)	KeyGen
AA	5	5
BB	6	6
C	5	5

However, after the key scanning and updating operation they keys for AA and C will be replaced to key generation 6 as well.

Conclusion

In conclusion, the inventive method assures that every row and item is re-encrypted with a valid key. More specifically this process, the so-called KeyLife process, is executed every time a row is inserted, updated or retrieved after a scanning operation. The key life value, defining the number of days a key is valid for each item, could differ for the items, and could typically be between 30 and 90 days. The scanning operation, checking the validity of the presently used keys, the so called KeyLife checking, is executed each time a new key generation is created.

We have now described the invention by means of a preferred method. However, several alternatives are possible and feasible. For example, the database items may have different sizes and structure, the inventive method may be operated on a single computer or on a computer network, different types of encryption may be used, different lifetimes for the keys may be set, etc. Such modifications must be considered to be within the

scope of the present invention, as it is defined by the enclosed claims.

CLAIMS

1. A method for encryption of the content in a database, comprising the steps of:

deciding the length of a time period to be used by the encryption method;

for each time period generating at least one encryption key to be used when entering new database items to the database;

storing information about the encryption key used for entering new items in the database in association with the item;

associating each encryption key with a life time value, indicating the number of time periods during which the key will be valid;

after entering a new time period, scanning the database to discover items with no longer valid encryption keys; and

replacing such discovered invalid keys with keys assigned to the current time period.

2. A method according to claim 1, wherein the items comprises rows in the database, each row comprising a column with information about the associated encryption key.

3. A method according to claim 1 or 2, wherein a specific lifetime value is associated with each item.

4. A method according to any one of the preceding claims, comprising the additional step of storing the replaced keys.

5. A method according to any one of the preceding claims, whereby the scanning of the database is performed as a background process.

6. A method according to any one of the preceding claims, whereby the scanning of the database is commenced and performed automatically after entering a new time period.

7. A method according to any one of the preceding claims, comprising the additional step of associating the items in the database with a timestamp indicating when it was last updated.

8. A method according to any one of the preceding claims, comprising the additional step of replacing the encryption key for an database item with a key generated for the present time period when the database item is updated.

9. A method according to any one of the preceding claims, wherein the keys are valid between 30 and 90 days.

10. A method according to any one of the preceding claims, wherein information about the encryption key used is stored as a hash value of the encryption key used, together with the encrypted data, in the database item.

11. A method according to any one of the preceding claims, wherein a value indicating the generation of the encryption key used for encrypting the database item is stored together with the encrypted data in the database item.

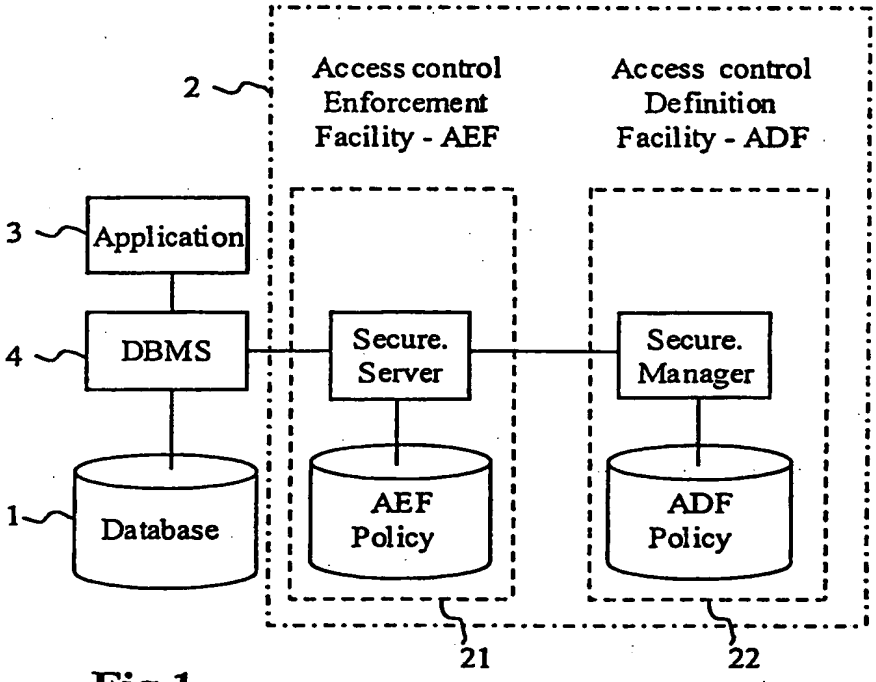

2
Access control Enforcement Facility - AEF
Access control Definition Facility - ADF
3
Application
4
DBMS
Secure. Server
Secure. Manager
1
Database
AEF Policy
ADF Policy
21
22

Fig 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/02219

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 12/14, G06F 17/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5915025 A (TAGUCHI ET AL), 22 June 1999 (22.06.99), column 3, line 56 - column 5, line 26; column 12, line 62 - column 13, line 11; column 13, line 35 - line 39, column 14, line 38 - column 16, line 43, figures 11-15, claims 1,13,17, abstract --	1-11
X	JP 11143780 A (HITACHI LTD) 1999-05-28 (abstract) World patents Index [on line]. London, UK.: Derwent Publications, Ltd. [retrieved on 2001-02-01]. Retrieved from: EPO WPI Database. DW199932, Accession No. 1999-376419, the whole document --	1-11
A	WO 9749211 A1 (ANONYMITY PROTECTION IN SWEDEN AB), 24 December 1997 (24.12.97), the whole document --	1-11

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 February 2001	28 -02- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Per Heimdal /OGU Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/00

International application No.
PCT/SE 00/02219

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5915025 A	22/06/99	JP 9258977 A	03/10/97
WO 9749211 A1	24/12/97	AU 724388 B	21/09/00
		AU 3282397 A	07/01/98
		BR 9710694 A	17/08/99
		CA 2257975 A	24/12/97
		CZ 9804158 A	14/07/99
		EP 0891661 A	20/01/99
		IL 127645 D	00/00/00
		JP 2000512785 T	26/09/00
		NO 985985 A	19/02/99
		SE 506853 C	16/02/98
		SE 9602475 A	21/12/97
		SK 174898 A	14/02/00

This Page Blank (uspto)